广播电视信息系统安全建设研究

李 萍
（北京市广播电视台，北京 100022）

摘 要：互联网的发展改变了各行各业的运作模式。在广播电视领域不断进步的过程中，也广泛依赖于信息技术，当前，广播电视领域信息系统建设已经较为成熟，但信息系统安全问题却层出不穷。信息安全在保障国家安全、社会和谐发展等方面发挥重要作用，因此，为了能够充分发挥信息系统作用，推动广播电视行业高效发展，必须针对当前存在的系统安全问题进行分析，予以优化。本文就对广播电视信息系统安全建设展开分析，供参考。

关键词：互联网；广播电视；信息系统；安全建设　　**中图分类号：**TP391　　**文献标识码：**A
文章编号：1671-0134（2021）12-158-03　　DOI：10.19483/j.cnki.11-4653/n.2021.12.051
本文著录格式：李萍 . 广播电视信息系统安全建设研究 [J]. 中国传媒科技，2021（12）：158-160.

导语

当前，我国广播电视在构建信息系统的同时，虽带来了便捷，推动行业革新进步，但安全问题也随之而来。导致广播电视信息系统产生安全问题的原因较多，病毒入侵、黑客攻击、操作系统漏洞，或者网络结构本就存在安全隐患等，都是导致信息系统无法正常运作的主客观因素。针对存在的种种安全问题，应采取有效策略予以完善，提高系统安全性，保障广播电视行业高质量发展。

1. 广播电视信息系统安全建设特点

现阶段，我国电视广播领域十分重视信息系统安全建设，将其看成是广电网络系统得以正常运作的保障，在建设时将信息化、数字化等技术作为重点组成。从整体而言，信息系统安全建设具有三大特点。[1] 其一，可操作性。信息系统安全建设具有较强的可操作性，要求系统内部功能需满足一体化设计，这也给之后的操作提供了极大便捷；其二，传输性。信息系统安全建设的传输性意味着系统采用多通道负载设计，有着较强的拓展能力，速率也呈线性增长趋势；其三，安全性。这一特点是信息系统安全建设的重中之重，广播电视行业之所以要进行安全设计，其目的就是为了给信息系统安全提供保障，安全性自然是建设核心。在建设过程中，系统会融入一些新型杀毒软件，同时融入多种安全策略组合，充分保障信息系统安全不受影响。

2. 广播电视信息系统安全体系具体结构

广播电视信息系统安全体系主要由管理层、运行层、技术层三个层次组成。[2] 其中，管理层包含信息安全有关法律常识、政策、管理机制、机构等，是整个系统的最高层，可以提供政策保障。运行层属于中间层次，其主要作用是给电视信息系统提供物质支撑，主要包含设备生产、应用、安装、维修等规范。技术层则主要是给系统提供技术支持，虽然内部内容比管理层、运行层少，但作用依旧不可忽视，其主要包含信息接收技术、信源技术、信通技术等。这三个层次在系统中都发挥不同作用，如果缺少其中任何一个层次信息系统安全都得不到保障，在三个层次密切结合的基础上，使系统运行更加有序规范，安全问题处理得井井有条。三个层次之间相互制约，但又相辅相成。

3. 广播电视信息系统安全建设问题的具体表现

3.1 病毒入侵

病毒入侵是广播电视信息系统最常见的安全问题之一。病毒就是指在系统程序中插入了会破坏系统功能或者会毁坏数据的指令、代码，在科技进步的同时，病毒形式也逐渐朝多元化方向发展，这使信息系统防不胜防。病毒会随编制者目的发生变化，有着先前性的特点，尤其是在近几年来，信息系统病毒种类越来越多，目前还在更新中。病毒的攻击目的和性质都各不相同，虽然针对传统病毒广播电视信息系统已经制定了防范措施，但对一些新型病毒信息系统预防工作做得并不乐观，这就导致系统安全岌岌可危。

3.2 黑客攻击

广播电视在我国社会和谐发展中发挥重要作用，是新闻传播的重要媒介，但从近些年来广播电视信息系统现状不难发现，黑客攻击时有发生，已经成为影响信息系统正常运行的主要因素，黑客攻击是导致信息安全不受保障的重要因素。[3] 黑客攻击程度不相等，如果攻击程度较轻，系统中的部分数据会被窃取，系统会出现短时间的故障；如果攻击程度较为严重，网络会被直接侵占，系统会被破坏。甚至有时一些黑客想通过广播电视传播谣言，给信息系统安全运行带来阻碍。

3.3 操作系统漏洞

操作系统在信息系统中占据重要地位，是硬件资源大平台，要想成功发挥软件作用就必须依靠操作系统，而且，操作系统是软硬件间的连接部分。其主要作用就

是配置内存、决定资源供需次序、控制输出入设备、操作网络文件系统等。然而，在操作系统运行时有时会突然被其他程序利用，导致原本正常发展的系统突然出现故障，给信息系统带来风险。但操作系统作为信息系统的关键组成，如果操作系统发生安全危害，则会直接影响到其他组织正常运行。

3.4 网络结构与设备存在安全隐患

我国广播电视行业的信息系统在运用时基本上都是使用混合型拓扑结构，在交换机或集线器等网络节点上本就存在一些安全隐患，但这些隐患在应用前并没有加以提出，在后续应用时安全问题逐渐凸显。其中，安全隐患最明显的地方就是硬件接口物理地址，其非常容易遭受网络攻击，这也是我国广播电视信息系统安全防范的难点。

3.5 硬件配置参差不齐

广播电视信息系统硬件配置呈现参差不齐的情况，大部分硬件配置都和当下需求相符，并不具备长远目光。这就使得硬件在使用一段时间后由于不能满足应用所需被淘汰，这时，就需重新更换硬件配置。当信息系统硬件配置缺乏科学性时，就会使系统风险防范与抵御能力较差。并且，有的设备即使超过了期限依旧在运行，在硬件设备老化后依旧工作，不但不会提高工作质量，反而会拉低系统整体工作效率，对广播电视事业发展非常不利。[4]

3.6 管理不够规范

广播电视信息系统管理不够规范主要体现在以下方面。第一，系统缺乏安全管理中心，无法对系统中的安全组件、硬件、软件等进行管理。在软件下发、硬件配置、病毒预防、安全控制等方面都存在不足，而这正是因为缺乏安全管理中心导致的。安全管理中心的主要工作就是对系统存在的多种安全问题进行分析、定位、解决，当缺乏管理中心时，自然无法提高系统安全性，导致一些安全问题逐渐滋生。第二，系统安全维护工作尚处于初步阶段，缺乏丰富经验。从具体的维护工作上就可以看出，采用的安全维护方法比较简单，也没有专业人才支持，导致系统安全维护水平不高。第三，虽然我国广播电视行业已经建立了网络安全管理部，也明确了其相关职责，但是由于具体工作的开展会受到内外部条件约束，导致在系统安全问题的监督、检测、响应方面机制并不完善。在没有机制支持下就使得系统信息安全得不到有力保障。第四，在展开网络信息安全管理工作时，一些管理人员缺乏安全意识，没有意识到安全管理的重要性与必要性。而且，用户在使用系统时也不具备较强的安全意识，往往存在错误使用习惯，给系统信息安全埋下巨大隐患。

3.7 安全评估检测引发安全问题

对广播电视信息系统来说，其安全问题的引发因素较多，除上述几种表现形式外，安全评估检测工作不足也会直接引发安全问题。我国广播电视领域对信息系统安全评估与检测工作并没有太多接触，在这方面比较空白。当广播电视展开评估检测工作时，也会受到能力、技术、设备等客观因素制约，尤其是对于地级市的广播电视系统来说，在系统安全评估检测工作的开展上难度更大。系统安全评估检测工作通常都需要借助网络安全检查工作实现，然而，在具体检测过程中涉及范畴比较狭窄，方法较为单一，只能发现系统存在的简单或显现安全问题，无法对系统进行深入检测。这就导致系统中的一些潜在隐性安全问题得不到发现，等到了后期运行时才会慢慢显现，但此时要想进行维修，难度和成本都比较高。

4. 广播电视信息系统安全建设的有效路径

4.1 应用病毒防护技术

要想在根本上避免病毒入侵，就必须应用病毒防护技术，对信息系统展开全方位保护。病毒进入信息系统的途径是网络，这也说明病毒必须在网络前提下才能进入广播电视信息系统。基于此，广播电视信息系统需全面实施网络安全策略，利用防病毒软件对进入系统内的信息进行扫描，把一切对系统有害的信息加以屏蔽。[5] 除此之外，还可以加强防火墙部署，这是抵御外界入侵的第一条防线，防火墙可以有效防止信息系统遭到病毒攻击。在防火墙运行时会探索到有关的权限检测对象，并结合信息系统当下运行状态给出提示，此时用户可以根据提示选择权限进行安装。有时防火墙也会自动检测权限，将对系统不利的权限全部屏蔽在外，以此来降低系统风险。不仅如此，防火墙还能够对错误指令加以警告，若系统中出现不良信息会立刻进行筛选，确保进入系统内的信息不具备威胁性。在安装防火墙时，则可以通过云计算技术升级系统建立自动升级功能，一旦系统发出升级指令防火墙就会自动升级，在极大程度提高系统运行可靠性。

4.2 应用加密技术和访问控制技术

加密技术可以说是广播电视信息系统安全保障的基石，通过对信息进行加密可以大大提高信息安全。在电视广播中有许多重要信息需得到储存，针对数据信息就可以采用加密技术，把数据信息经过加密钥匙、函数加以转换，生成无意义密文，接收方需要将该密文进行解密还原成明文才能查看该数据。这种加密方法比较适合用在广播电视信息系统之中，可以确保重要数据信息不被非法查阅。访问控制技术是避免黑客入侵的有效策略，主要用于路由器或交换机等设备上，可以对网络访问权限进行控制。在广播电视信息系统中应用该技术则可以对系统访问者的权限予以控制，在确保安全的前提下允许访问者进入。在实际应用时，通过配置路由器中的访问控制列表，可以生成一个完善的防火墙，对进出入设备 IP 数据进行筛选，把一些可能存在入侵倾向的访问权限隔绝在外，防止黑客非法入侵。

4.3 构建结构防护框架

在广播电视信息系统安全建设过程中，还应构建结构防护框架，才能预防一系列安全问题发生。广播电视系统建设重点应转移一部分到框架构建上，确保可以在结构化保护理念上展开具体的构建工作。在此基础上，可以使网络边缘全面覆盖信息系统，使信息系统整体在网络保护范畴内。在信息系统访问路径的定义方面，各接口参数与相关安全协议都应保持健全。为了能够确保客体访问效果，还应做好互联网访问应用路径处理工作，从而使广播电视信息系统框架的核心可以得到有效保护，提高系统整体安全效果。[6]

4.4 加强软硬件防范

对于广播电视信息系统来说，软硬件都占据核心地位，如果一台终端设备被病毒感染，服务器或其他终端设备被影响的概率也会随之提升。在进行硬件安全防范过程中，可以通过用户行为管理，制定用户操作规范的方式实现对用户行为的约束。对于硬件设备上的一些不实用服务端口应及时关闭，且禁止随便安装系统软件。对广播电视信息系统账号进行管理时，无论从认证、授权还是口令等方面都采用多元化设置。针对一些已经老化的硬件设备，广播电视领域必须及时更换，切勿抱有侥幸心理。[7]广播电视信息系统的软件主要包含操作系统、数据库等，为避免软件出现安全故障，在选择软件时尽量选择可靠性较强的软件，并选择本就具有相关安全开发保障的软件。在正式应用软件的第一时间要及时下达广播电视平台软件安全规范。对软件商家所发布的漏洞信息需立即跟踪，结合漏洞实际情况制定科学合理的补救方案，提高软件应用稳定程度。

4.5 健全系统管理制度

广播电视信息系统安全建设离不开管理制度，当拥有健全的系统管理制度后可以给整个建设过程提供有力支撑。应强化信息系统运行环境，对互联网终端应用情况予以监督，避免出现操作不当的现象影响系统安全运行。并且，对重要信息数据应进行备份处理，还应明确奖惩机制。对在管理工作中表现较好的员工，应给予物质或精神奖励，而对屡犯错误且不知悔改的管理人员要做出相应惩罚，使奖惩机制震慑性得到充分发挥，确保信息系统安全管理工作切实落实。此外，为了提高制度实操性，可以针对现有的应急预案加以完善，通过互联网、计算机等技术手段建立集设备运行监测、应急指挥、安全播出、预警发布等功能为一体的保障体系，全方面提高电视广播信息系统安全水平。

4.6 强化安全评估检测工作力度

安全评估检测工作贯穿于广播电视信息系统全程，如果不进行安全评估检测就无法判断系统是否具备安全性。系统安全评估检测工作深度要得到加强，在检测时一定要扩大检测范围，采用多元化方法展开评估，确保系统潜在安全问题可以得到发掘，为后续高效运作提供保障。[8]在实际的评估检测过程中，要对系统设备的运作情况、用户行为、网络边缘数据行文等充分检测，当发现异常时需及时提出，切勿隐瞒，对隐瞒所造成的严重后果要落实到当事人头上。同时，还要对用户行为进行审计评估，如登录情况、核心业务操作情况、配置修改等。在评估检测时要做好对应记录工作，把具体的检测评估对象、时间、地点、事件、类型等全部记录清楚，必要时可以提供有力依据。[9]

结语

综上所述，广播电视信息系统安全体系由管理层、运行层、技术层组成，三者缺一不可。从当前广播电视信息系统安全现状来看依旧存在许多问题，本文阐述了七大问题，分别是病毒入侵、黑客攻击、操作系统漏洞、网络结构与设备存在安全隐患、硬件配置参差不齐、管理不够规范及安全评估检测不足。为推动广播电视信息系统高效有序运作，可以通过应用病毒防护技术、应用加密技术和访问控制技术、构建结构防护框架、加强软硬件防范、健全系统管理制度、强化安全评估检测工作力度的策略实现，为我国广播电视领域可持续发展贡献力量。媒

参考文献

[1] 高小清 . 广播电视信息系统网络安全风险与策略 [J]. 通讯世界，2019（11）：51-52.

[2] 孟莲蓉 . 广电某信息系统的安全性与保密性设计 [J]. 广播电视信息，2016（S1）：102-103.

[3] 邱福如 . 基于广电网络融合终端信息安全系统的应用研究 [J]. 无线互联科技，2020（16）：15-16.

[4] 方珉晔 . 广播电视信息传输系统安全性的维护 [J]. 西部广播电视，2016（17）：232.

[5] 陈乐 . 浅析云技术时代广播电视信息化平台建设和应用 [J]. 信息周刊，2019（41）：1.

[6] 张俐 . 浅谈广播电视播控技术安全管理现状及对策 [J]. 数字化用户，2019（4）：59.

[7] 徐程 . 电视播出系统网络信息与数据安全研究 [J]. 西部广播电视，2019（19）：255-256.

[8] 任晓炜 . 广播电视信息系统网络安全加固方法研究 [J]. 广播与电视技术，2019（2）：8-12.

[9] 彭杰 . 维护广播电视信息传输系统安全性的方法 [J]. 中国传媒科技，2014（6）：129.

作者简介：李萍（1978-），女，青海西宁，硕士，高级工程师，研究方向：广播电视信息系统建设、运行维护。

（责任编辑：张晓婧）